Inventiones math. 8, 83 – 97 (1969)

On Isometries of Inner Product Spaces

JOHN MILNOR (Cambridge, Mass.)

By an *inner product space* V will be meant a finite dimensional vector space V over a field F together with a non-degenerate, bilinear, F-valued inner product $\langle u, v\rangle$ which is either symmetric or skew symmetric. The group of *isometries* t of V (that is F-linear automorphisms satisfying the identity $\langle t u, t v\rangle = \langle u, v\rangle$) will be denoted by $O(V)$ in the symmetric case and by $Sp(V)$ in the skew case. (Of course if F has characteristic 2 then this distinction disappears.)

The problem of classifying all conjugate classes in the group $O(V)$ or $Sp(V)$, or equivalently the problem of classifying, up to isomorphism, all pairs V, t consisting of an inner product space and an isometry, was solved by Williamson [16], assuming that the field F is perfect of characteristic $\neq 2$. (See also Wall [15].) We will present a slightly more perspicuous version of this classification in § 3. Our point of view is similar to that of Cikunov [3–6].

The first two sections of this paper are concerned with a more specialized discussion of isometries with irreducible minimal polynomial. If F is a local field of characteristic $\neq 2$, then it is shown that $O(V)$ contains at most one conjugate class having a given irreducible minimal polynomial. This verifies a conjecture of Levine. The proof involves a study of the behavior of quadratic forms over local fields under restriction of the field (§ 2.3).

The results of § 2 will be applied in a forthcoming paper [11] by Levine to the study of codimension 2 knots. (See also [10, 12].) I am indebted to Levine for many useful discussions.

§ 1. The Case of an Irreducible Minimal Polynomial

Let V be a symmetric inner product space (or briefly a *quadratic space*[1]) of dimension n over F, and let t be a fixed element of the orthogonal group $O(V)$. We will frequently think of V as a finitely generated module over the polynomial ring $F[t]$ in one indeterminate. The *minimal polynomial* $m(t)$ is defined to be the monic polynomial of lowest degree in $F[t]$ for which $m(t)V = 0$. If $m(t)$ is irreducible, of degree say k, then

1. In the characteristic 2 case, the term "quadratic space" is usually given a different meaning.

we can also think of V as a vector space of dimension n/k over the field

$$E = F[t]/m(t)F[t].$$

Clearly E is a finite extension field, of degree k over F.

The image in E of the indeterminate t will be denoted by τ. Thus $E = F(\tau)$, and the isometry t of V is just the left multiplication transformation $v \mapsto \tau v$.

Lemma 1.1. *There is a unique automorphism $e \mapsto \bar{e}$ of E over F which carries τ to τ^{-1}. If E is separable over F, then the vector space V over E admits one and only one hermitian inner product*

$$u \cdot v = \overline{v \cdot u},$$

E-linear in the first variable, which is related to the original F-valued inner product by the identity

$$\langle u, v \rangle = \operatorname{trace}_{E/F}(u \cdot v). \tag{1}$$

For fixed $m(t)$, the isomorphism class of this resulting hermitian inner product space H determines the isomorphism class of V, t completely.

Proof. Note the identity $\langle f(t)u, v \rangle = \langle u, f(t^{-1})v \rangle$ which holds for any $f(t) \in F[t]$. Applying this identity to the minimal polynomial, we see that the linear transformation $t^k m(t^{-1})$ annihilates V, and therefore that the polynomial $t^k m(t^{-1})$ must be a multiple of $m(t)$. Substituting τ for t, this proves that $m(\tau^{-1}) = 0$. Therefore there is an automorphism, $e \mapsto \bar{e}$, of E over F which carries τ to τ^{-1}.

Note the identity

$$\langle e\,u, v \rangle = \langle u, \bar{e}\,v \rangle. \tag{2}$$

We will next show that there is one and only one inner product $u \cdot v \in E$ which satisfies the identity (1) and is E-linear in the first variable.

For fixed u and v consider the F-linear map

$$e \mapsto L(e) = \langle e\,u, v \rangle$$

from E to F. Since E is separable over F there is one and only one element e' of E such that

$$\operatorname{trace}(e\,e') = L(e)$$

for all e. (Compare [9, p. 211].) We define $u \cdot v$ to be this element e', so that the symbol $u \cdot v$ is defined by the equation

$$\operatorname{trace}(e(u \cdot v)) = \langle e\,u, v \rangle \tag{3}$$

for all e. In particular, taking $e = 1$ we obtain the required formula (1).

Proof that $u \cdot v$ is linear in the first variable. The identity

$$u_1 \cdot v + u_2 \cdot v = (u_1 + u_2) \cdot v$$

is easily verified. Now substitute $e_1 e_2$ for e in Eq. (3), or alternatively substitute e_1 for e and $e_2 u$ for u in (3). Comparing the two results we obtain

$$\operatorname{trace}(e_1 e_2 (u \cdot v)) = \operatorname{trace}(e_1((e_2 u) \cdot v))$$

for all e_1, and therefore

$$e_2 (u \cdot v) = (e_2 u) \cdot v, \tag{4}$$

as required.

Proof of Uniqueness. Given any inner product $u \cdot v$ satisfying (4) and (1), it follows that

$$\operatorname{trace}(e(u \cdot v)) = \operatorname{trace}((e u) \cdot v) = \langle e u, v \rangle .$$

Thus (4) and (1) imply Eq. (3) which uniquely characterizes the symbol $u \cdot v$.

Proof that $v \cdot u = \overline{u \cdot v}$. The identity $\operatorname{trace} e = \operatorname{trace} \bar{e}$, together with (3) and (2), implies that

$$\operatorname{trace}(e\, \overline{u \cdot v}) = \operatorname{trace}(\bar{e}\, u \cdot v) = \langle \bar{e} u, v \rangle = \langle u, e v \rangle$$

$$= \langle e v, u \rangle = \operatorname{trace}(e(v \cdot u)).$$

Since this holds for all e, we obtain $\overline{u \cdot v} = v \cdot u$, which completes the proof.

The polynomials $m(t)$ which can occur in 1.1 can be easily characterized as follows. A polynomial

$$m(t) = a_0 t^k + a_1 t^{k-1} + \cdots + a_k$$

of degree k over F will be called *ε-symmetric* if its coefficients satisfy

$$a_i = \varepsilon a_{k-i}$$

for some fixed element ε of F. Clearly ε^2 must be $+1$ so ε can only be ± 1.

Lemma 1.2. *The minimal polynomial $m(t)$ of § 1.1 must be ε-symmetric. Conversely given any monic ε-symmetric separable irreducible polynomial $m(t)$, and any hermitian inner product space H over the field*

$$E = F[t]/m(t)F[t],$$

the inner product $\operatorname{trace}_{E/F} u \cdot v$ with values in F is symmetric and non-degenerate, and thus makes H into a quadratic space H_F over F. Left multiplication by t gives rise to an isometry of H_F with minimal polynomial equal to $m(t)$.

The proof is straightforward.

Remark 1.3. In general an ε-symmetric polynomial $m(t)$ must have even degree and must have $\varepsilon=+1$, the only exceptions being the polynomials $t-1$ and $t+1$ and their multiples. For if $\varepsilon\neq+1$ then $m(1)=0$ so that $m(t)$ must be a multiple of $t-1$, while if the degree is odd with $\varepsilon=+1$ then $m(-1)=0$ so that $m(t)$ must be a multiple of $t+1$.

Remark 1.4. The hypothesis that E is separable over F is needed only to insure that the trace homomorphism from E to F is non-zero. If E is inseparable over F we can still choose some fixed non-zero F-linear homomorphism which satisfies the identity $h(\bar{e})=h(e)$. Using h in place of the trace, the results of § 1 (and of §§ 2, 3) extend immediately to the inseparable case. Compare W. Scharlau: Zur Pfisterschen Theorie der quadratischen Formen. Inventiones math. **6**, 327–328 (1969).

Remark 1.5. Completely analogous results hold in the case of an isometry of a skew symmetric inner product space W. In fact the skew case can be reduced to the symmetric case as follows. Given a fixed element $t\in Sp(W)$, if t has no eigenvalues of ±1, then the operator $\Delta=t-t^{-1}$ maps W isomorphically onto itself. We introduce a new inner product $u\cdot v$ on W by the rule

$$u\cdot v=\langle \Delta u, v\rangle,$$

thus making W into a symmetric inner product space W^s. Clearly $(tu)\cdot(tv)=u\cdot v$, so that t is an isometry of W^s also. Thus there is a one-to-one correspondence between isometries of skew inner product spaces and isometries of symmetric inner product spaces, providing only that we avoid eigenvalues of ±1.

In order to exploit Lemmas 1.1 and 1.2 we must be able to classify hermitian inner product spaces over E. Fortunately these are somewhat easier to classify than quadratic spaces. (Compare Jacobson [7].) We will assume that $E\neq F$ so that the involution $e\mapsto\bar{e}$ is not the identity.

First recall that any hermitian space H over E possesses an orthogonal basis $v_1,\ldots,v_r$. In other words the inner product matrix of H can be diagonalized. Clearly the diagonal entries

$$k_i=v_i\cdot v_i$$

must belong to the fixed field K of the involution $e\mapsto\bar{e}$ of E over F. If we multiply the basis vector v_i by an element of the multiplicative group $\dot{E}$, note that the corresponding diagonal entry $v_i\cdot v_i$ is multiplied by an element of $\mathrm{norm}_{E/K}\dot{E}$.

Example 1. If E is a finite field then the norm is surjective and it follows that the rank r of H forms a complete invariant. (Compare Cikunov [6].)

One easily defined invariant of a hermitian space is the *determinant* of a representative inner product matrix, which is well defined as an element of the quotient group $\dot{K}/\mathrm{norm}_{E/K}\,\dot{E}$.

Example 2. If the rank r is 1, then clearly the determinant of H forms a complete invariant.

Example 3. If F is a local field (that is if F is complete under a discrete valuation with finite residue class field), then $\dot{K}/\mathrm{norm}_{E/K}\,\dot{E}$ has precisely two elements ([13, p. 167] or [1, p. 222]). In this case it is easily verified that the rank and determinant form a complete set of invariants.

Example 4. If K is the field of real numbers, so that E is the field of complex numbers, then again $\dot{K}/\mathrm{norm}\,\dot{E}$ has two elements. In this case it is well known that the rank and index form a complete set of invariants. (Following Marston Morse, the *index* of a hermitian space means the number of negative entries in a diagonalized inner product matrix.) Thus the rank and determinant do not suffice in this case.

Example 5. If E is a finite extension of the field of rational numbers, then for each embedding ρ of K in the field R of real numbers which does not extend to an embedding of E in R one can define an index I_ρ of the hermitian space H over E. These indices, together with the rank r and determinant d, form a complete set of invariants. (See Landherr [8].) They are subject only to the relations $0 \leqq I_\rho \leqq r$ and

$$(-1)^{I_\rho} = \rho(d)/|\rho(d)|\,.$$

§ 2. Local Fields: A Conjecture of Levine

Suppose that F is either the field of real numbers or a local field of characteristic $\neq 2$. (Compare Example 3 of § 1.) Then we will prove:

Theorem 2.1. *If two isometries t and t' of a quadratic space V over F have the same irreducible minimal polynomial, then t is conjugate to t' in the orthogonal group $O(V)$.*

In other words the minimal polynomial, together with the invariants needed to characterize V, form a complete set of invariants for the pair V, t.

This verifies a conjecture which was formulated, and proved in a number of special cases, by Levine (unpublished).

Note that the corresponding statement for an arbitrary field would definitely be false (e.g. for the field of rational numbers).

Proof of 2.1 *for the Real Field.* If we exclude the uninteresting case $m(t)=t\pm 1$, then a complete set of invariants for the pair (V, t) is provided by the rank and index of the associated Hermitian inner product space H over C. (Compare Example 4 of § 1.) But clearly $2\,\mathrm{rank}_C H = \mathrm{rank}_R V$, $2\,\mathrm{index}_C H = \mathrm{index}_R V$, so that these invariants are completely determined by the invariants of V.

The proof of 2.1 for local fields is more difficult, and will occupy the rest of § 2.

First consider a finite separable extension K of an arbitrary field F. Choosing a basis $k_1, \ldots, k_p$ for K over F, the *discriminant*, $\mathrm{discr}(K/F)$, is defined to be the element of the quotient group $\dot{F}/\dot{F}^2$ which is represented by the determinant of the matrix $(\mathrm{trace}_{K/F}(k_i k_j))$.

Any quadratic space W of rank s over K can be made into a quadratic space of rank ps over F by introducing the F-valued inner product $\mathrm{trace}_{K/F}\langle v, w\rangle$.

Lemma 2.2. *The determinant of the resulting quadratic space W_F over F is related to the original determinant in $\dot{K}/\dot{K}^2$ by the equation*

$$\det W_F = (\mathrm{discr}\, K/F)^s \,\mathrm{norm}_{K/F}(\det W),$$

which holds in $\dot{F}/\dot{F}^2$.

Proof. First suppose that W has rank 1, with basis vector w. Let

$$\langle w, w\rangle = c \in \dot{K}.$$

Then W_F has basis $k_1 w, \ldots, k_p w$, and inner product matrix $(\mathrm{trace}(c\, k_i\, k_j))$. Setting

$$c\, k_i = \sum a_{ih}\, k_h$$

with $a_{ih} \in F$, this inner product matrix can be considered as the product of the matrix (a_{ih}), with determinant equal to

$$\mathrm{norm}(c) \equiv \mathrm{norm}\det W \mod \dot{F}^2$$

(see [14, p. 130]), and the matrix $(\mathrm{trace}(k_h k_j))$ with determinant equal to $\mathrm{discr}(K/F)$.

The proof when rank $W>1$ is similar. It is only necessary to express W as an orthogonal sum of one dimensional spaces[2], and then to use the fact that the determinant of an orthogonal sum equals the product of the determinants. This proves 2.2.

Now suppose that F is a local field of characteristic $\neq 2$. Then a complete set of invariants for a quadratic space V over F is provided by the rank $n \geqq 1$, the determinant $\det V \in \dot{F}/\dot{F}^2$, and the Hasse symbol

2. In characteristic 2 this may not be possible, but the lemma can then easily be proved by an alternative argument.

$S(V) \in \{\pm 1\}$. (Compare O'Meara [13, § 63B]. These are subject only to the relation that $S(V)$ must be equal to the Hilbert symbol $(\det V, -1)$ whenever either $n=1$, or $n=2$ and $\det V = -\dot{F}^2$.)

Theorem 2.3. *Let V and W be two quadratic spaces over a separable extension K of the local field F. If V and W have the same rank and determinant but are not isomorphic, then the corresponding quadratic spaces V_F and W_F over F also have the same rank and determinant but are not isomorphic.*

(For the definition of V_F see 2.2.)

In other words, if rank V = rank W, and $\det V = \det W$, but $S(V) \neq S(W)$, then it follows that $S(V_F) \neq S(W_F)$.

The proof of 2.3 will be interrupted by three lemmas.

Lemma 2.4. *In order to prove Theorem 2.3 for a given field extension $K \supset F$ it is sufficient to produce one example of a pair of quadratic spaces V^0 and W^0 over K with the same rank and determinant, but with $S(V_F^0) \neq S(W_F^0)$.*

Proof. Since V_F^0 is not isomorphic to W_F^0, it follows that V^0 is not isomorphic to W^0 and hence $S(V^0) \neq S(W^0)$.

Now given V and W, as in 2.3, note that the orthogonal sum $V \oplus V^0$ is isomorphic to $W \oplus W^0$. This is true since both sums have the same rank, determinant, and Hasse symbol, using the identity

$$S(V \oplus V^0) = S(V) S(V^0) (\det V, \det V^0).$$

Hence $V_F \oplus V_F^0 \cong W_F \oplus W_F^0$. Now using the corresponding formula for the Hasse symbol of an orthogonal sum over F, and using 2.2, we see that $S(V_F) \neq S(W_F)$ as required.

The proof of 2.3 will be divided into five cases, of which the first is crucial.

Case 1. *Suppose that K contains an element k_0 whose norm in F is not a square.* Then we can choose $b \in \dot{F}$ so that the Hilbert symbol $(b, \text{norm } k_0)$ equals -1. (Compare [13, p. 166].) Let $V(k, -bk)$ be the quadratic space of rank 2 over K whose inner product matrix is

$$\begin{pmatrix} k & 0 \\ 0 & -bk \end{pmatrix}.$$

Lemma 2.5. *The Hasse symbol of $V(k, -bk)_F$ is equal to $(b, \text{norm } k)$ times a factor $(b, \text{discr } K/F)(-b, -b)^{p(p+1)/2}$ which does not depend on the choice of k.*

Thus choosing either $k=1$ or $k=k_0$ we will obtain two quadratic spaces over K with the same rank 2 and the same determinant $-b$, but so that the corresponding quadratic spaces over F have different Hasse symbols. This will complete the proof in Case 1.

Proof of 2.5. The space $V(k, -b\,k)$ splits as an orthogonal sum $V' \oplus V''$ where V' has determinant k and V'' has determinant $-b\,k$. Choose an orthogonal basis for the quadratic space V'_F, and let $a_1, \ldots, a_p$ be the diagonal entries for the resulting diagonal inner product matrix. Then a corresponding diagonal matrix for V''_F has diagonal entries $-b\,a_1, \ldots, -b\,a_p$. By definition the Hasse symbol S' of V'_F is equal to $\prod_{i \leqq j} (a_i, a_j)$, and the Hasse symbol S'' of V''_F is equal to

$$\prod_{i \leqq j} (-b\,a_i, -b\,a_j) = \prod_{i \leqq j} \big((a_i, a_j)(-b, a_j)(a_i, -b)(-b, -b)\big)$$

$$= S'(-b, a_1 \ldots a_p)^{p+1}(-b, -b)^{p(p+1)/2}.$$

Hence the Hasse symbol

$$S'S''\big(a_1 \ldots a_p, (-b)^p a_1 \ldots a_p\big)$$

of $V'_F \oplus V''_F \cong V(k, -b\,k)_F$ is equal to

$$(-b, a_1 \ldots a_p)^{2p+1}(-1, a_1 \ldots a_p)(-b, -b)^{p(p+1)/2}$$

$$= (b, a_1 \ldots a_p)(-b, -b)^{p(p+1)/2},$$

using [13, p. 166]. Substituting

$$a_1 \ldots a_p = \det V'_F = \operatorname{discr}(K/F) \operatorname{norm} k$$

we obtain the required formula. This completes the proof of 2.5, and hence of Case 1 of Theorem 2.3.

Case 2. *Suppose that K has degree $p=2$ over F.* Then norm $\dot{K}$ has index 2 in $\dot{F}$ while $\dot{F}^2$ has index $\geqq 4$ in $\dot{F}$. (Compare [13, pp. 163, 167].) So the hypothesis of Case 1 is certainly satisfied.

Case 3. *Suppose that K has odd degree p over F.* Choosing any element $c \in \dot{F}$ which is not a square, the p-th power $c^p \in \operatorname{norm} K$ will not be a square either. So the hypothesis of Case 1 is again satisfied.

Case 4. *Suppose that the extension K of F is such that no intermediate field (other than F itself) is abelian over F.*

Lemma 2.6. *In this case the image* $\operatorname{norm}_{K/F} \dot{K}$ *is equal to the entire multiplicative group* $\dot{F}$.

So in this case again the hypothesis of Case 1 is satisfied.

The proof of 2.6 will be based on the norm residue isomorphism of local class field theory. First suppose that K is a Galois extension of F

with group G. Then we have the isomorphism

$$\dot{F}/\text{norm}\,\dot{K} \cong G/[G, G].$$

(See [1, pp. 222, xv, xxii].) But G is equal to its commutator subgroup, since no intermediate field is abelian over F.

If K is not a Galois extension then we can embed K in a Galois field Ω over F. Let G be the group of Ω over F and H the group of Ω over K. Then we have the commutative diagram

$$\begin{array}{ccc} H/[H,H] & \longrightarrow & G/[G,G] \\ \downarrow \cong & & \downarrow \cong \\ \dot{K}/\text{norm}_{\Omega/K}\,\dot{\Omega} & \xrightarrow{\text{norm}_{K/F}} & \dot{F}/\text{norm}_{\Omega/F}\,\dot{\Omega} \to \dot{F}/\text{norm}_{K/F}\,\dot{K} \to 1. \end{array}$$

(See [1, pp. 217, 224], together with [2, p. 255].) But the top homomorphism is surjective, since otherwise H and $[G, G]$ would generate a proper subgroup of G, corresponding to an abelian intermediate field. Hence every element in $\dot{F}$ is a norm from $\dot{K}$. This completes the proof in Case 4.

General Case. For any finite separable extension $F \subset K$ we can choose a tower of intermediate fields

$$F = F_0 \subset F_1 \subset \cdots \subset F_q = K$$

so that each F_{i+1} is either an abelian extension of F_i with prime degree, or else an extension with no abelian intermediate field. Starting with non-isomorphic quadratic spaces V and W over F_q with the same rank and determinant, we see by induction on i that $V_{F_{q-i}}$ is not isomorphic to $W_{F_{q-i}}$; using Cases 2, 3, 4. This completes the proof of Theorem 2.3.

Now consider a quadratic extension E of K and a hermitian inner product space H over E. We continue to assume that K is finite and separable over a local field F of characteristic $\neq 2$. Recall that the determinant of H is an element of a group $\dot{K}/\text{norm}\,\dot{E}$ with precisely two elements. Recall also that the inner product $\text{trace}_{E/F}(u \cdot v)$ makes H into a quadratic space H_F over F.

Theorem 2.7. *If two hermitian spaces H and H' over E have the same rank but different determinants, then the corresponding quadratic spaces H_F and H'_F have the same rank and determinant but different Hasse symbols.*

Proof. Clearly it suffices to consider the case where H has rank 1 over E. Let (k) be the inner product matrix of H. If $E = K[\sqrt{b}]$, then using 1 and $\sqrt{b}$ as basis for E over K we see that H_K has inner product

matrix

$$\begin{pmatrix} 2k & 0 \\ 0 & -2bk \end{pmatrix}.$$

Thus the determinant of H_K is $-b$, which is independent of the choice of k. But

$$S(H_K) = (2k, 2k)(2k, -2bk)(-2bk, -2bk)$$
$$= (2k, b)(-b, -b).$$

Since b is not a square in K, this clearly does depend on the choice of k.

Now in order to pass from H_K to H_F we need only apply 2.2 and 2.3. This completes the proof of 2.7.

We are now ready to prove Theorem 2.1 in the separable case. Given two isometries t and t' of V with the same irreducible minimal polynomial, form the corresponding hermitian spaces H and H', using § 1.1. If t is not conjugate to t' in $O(V)$, then the pair (V, t) is not isomorphic to (V, t'), hence H is not isomorphic to H'. But clearly rank H = rank H', so it follows that $\det H \neq \det H'$. Therefore H_F is not isomorphic to H'_F by 2.7. But $H_F = H'_F = V$. This contradiction completes the proof, assuming that K is separable over F.

The proof in the inseparable case is completely analogous. It is only necessary to make use of Remark 1.4, and the fact that a purely inseparable extension has odd degree. (Recall that we exclude the characteristic 2 case.) Details will be left to the reader.

Remark 2.8. Given a fixed quadratic space V of dimension n over F, how can we decide whether or not a given irreducible polynomial $m(t)$ actually occurs as the minimal polynomial for some isometry of V? We exclude the trivial case $m(t) = t \pm 1$. If F is a local field of characteristic $\neq 2$ then necessary and sufficient conditions are that $m(t)$ be monic, symmetric (compare 1.3), with even degree k dividing n, and with $\det V = (m(1)m(-1))^{n/k}\dot{F}^2$. The proof is not difficult.

§ 3. The Classification of Arbitrary Isometries

Let t be an isometry of the inner product space V. For each monic irreducible factor $p(t)$ of the characteristic polynomial of t, let $V_{p(t)}$ denote the *$p(t)$-primary subspace*, consisting of all v with $p(t)^i v = 0$ for large i. Thus the vector space V is the direct sum of the sub vector spaces $V_{p(t)}$.

Define the "dual" of the monic irreducible polynomial

$$p(t) = t^k + a_1 t^{k-1} + \cdots + a_k$$

to be the monic irreducible polynomial

$$p^*(t) = (a_k t^k + a_{k-1} t^{k-1} + \cdots + 1)/a_k.$$

Lemma 3.1. *The $p(t)$-primary subspace $V_{p(t)}$ is orthogonal to the $q(t)$-primary subspace unless the polynomial $p(t)$ is "dual" to $q(t)$.*

In particular, $V_{p(t)}$ is orthogonal to itself unless $p(t)=p^*(t)$. In other words, in the terminology of § 1.2 and § 1.3, the space $V_{p(t)}$ is orthogonal to itself unless the polynomial $p(t)$ is ε-symmetric, where ε can be either $+1$ or -1.

Proof. If i is sufficiently large then the identity

$$\langle u, p(t^{-1})^i v\rangle = \langle p(t)^i u, v\rangle = \langle 0, v\rangle$$

for $u \in V_{p(t)}$ shows that $V_{p(t)}$ is orthogonal to $p(t^{-1})^i V$. But if $q(t) \neq p^*(t)$ then the correspondence

$$v \mapsto p(t^{-1})v = a_k t^{-k} p^*(t) v$$

maps the subspace $V_{q(t)}$ isomorphically onto itself. Hence $V_{p(t)} \perp V_{q(t)}$ as asserted.

Following Cikunov, we divide the primary subspaces into three classes, of which the first two are more interesting.

Case 1. The polynomial $p(t)$ is self dual, $p(t)=p^*(t)$, of degree $\geqq 2$.

Case 2. $p(t)$ is self dual of degree 1, and hence is equal to $t \pm 1$. In Case 2 we will always assume that F has characteristic $\neq 2$. (Compare [15, § 3].)

Case 3. $p(t)$ is not self-dual.

In Cases 1 and 2 note that the primary summand $V_{p(t)}$ splits off as an orthogonal direct summand of V. Furthermore:

Theorem 3.2. *In Cases* 1 *and* 2 *the space $V_{p(t)}$ itself splits as an orthogonal direct sum $V^1 \oplus V^2 \oplus V^3 \oplus \cdots$ where each V^i is annihilated by $p(t)^i$, but is free when considered as a module over the quotient ring $F[t]/p(t)^i F[t]$. This splitting is unique up to isomorphism (assuming that the characteristic is $\neq 2$ in Case 2).*

In order to proceed further in Case 1 we note by § 1.3 that the polynomial $p(t)$ must be symmetric and of even degree $2d$. We will make use of the rational function $s(t)=p(t)/t^d$ which satisfies the identity $s(t)=s(t^{-1})$, and hence defines a self-adjoint transformation of V:

$$\langle s(t)u, v\rangle = \langle u, s(t)v\rangle .$$

Assume that the inner product $\langle u, v\rangle$ is symmetric. (Compare § 1.5.)

Theorem 3.3. *In Case* 1, *if the polynomial $p(t)$ is separable, then for each V^i the associated vector space*

$$H^i = V^i / p(t) V^i$$

over the field $E = F[t]/p(t)F[t]$ *admits one and only one hermitian inner product* $(u) \cdot (v)$ *which satisfies the identity*

$$\langle s(t)^{i-1} u, v \rangle = \mathrm{trace}_{E/F}(u) \cdot (v)$$

for all u *and* v *in* V^i. *The sequence consisting of the isomorphism classes of these hermitian inner product spaces* $H^1, H^2, \ldots$ *forms a complete invariant for the pair* $V_{p(t)}, t | V_{p(t)}$.

Of course the hypothesis of separability is not really essential. (Compare § 1.4.)

Remark. If we ignore the isometry t, and think of V^i only as a quadratic space over F, then its structure can be described quite simply as follows. If i is even then V^i contains a totally isotropic subspace $s(t)^{i/2} V^i$ of half the dimension; hence V^i splits as an orthogonal sum of hyperbolic planes ([13, p. 99]). If i is odd then a similar argument shows that V^i splits as an orthogonal sum of a quadratic space isomorphic to $(H^i)_F$ (notation as in § 1.2) and a number of hyperbolic planes.

The situation in Case 2 is similar. Let Δ denote the operator $t - t^{-1}$ which is skew self-adjoint,

$$\langle \Delta u, v \rangle = -\langle u, \Delta v \rangle .$$

Let ε stand for $+1$ or -1 according as the inner product $\langle u, v \rangle$ is symmetric or skew.

Theorem 3.4. *In Case* 2 *the associated vector space* $V^i/p(t)V^i$ *over* F *admits an inner product*

$$(u) \cdot (v) = \langle \Delta^{i-1} u, v \rangle$$

which is well defined, non-degenerate, and $(-1)^{i-1}\varepsilon$*-symmetric. The sequence consisting of the isomorphism classes of these inner product spaces* $V^i/p(t)V^i$, $i = 1, 2, 3, \ldots$, *forms a complete invariant for the isomorphism class of* $V_{p(t)}, t | V_{p(t)}$.

Thus for half of the values of i we obtain a nontrivial invariant: namely a symmetric inner product space over F. For the remaining values of i we obtain only a skew inner product space, which is completely characterized by its rank.

Finally we come to Case 3. If $p(t) \neq p^*(t)$ then $V_{p(t)}$ is orthogonal to itself, but $V_{p(t)} \oplus V_{p^*(t)}$ splits off from V as an orthogonal direct summand. Choosing a basis for $V_{p(t)}$ and a dual basis for $V_{p^*(t)}$, the inner product matrix and the matrix of the linear transformation $t | V_{p(t)} \oplus V_{p^*(t)}$ take the forms

$$\begin{pmatrix} 0 & I \\ \pm I & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} T & 0 \\ 0 & (T')^{-1} \end{pmatrix}$$

respectively. Hence the similarity class of $t|V_{p(t)}$ forms a complete invariant in this case.

Thus Case 3 is uninteresting. We return to Case 1. The proofs will be given in outline only.

Proof that there exists an orthogonal splitting

$$V_{p(t)} = V^1 \oplus V^2 \oplus \cdots \oplus V^m$$

with each V^q *free over* $F[t]/(p(t)^q)$. First choose a not necessarily orthogonal splitting $V_{p(t)} = W_1 \oplus \cdots \oplus W_m$ with W_q free over $F[t]/(p(t)^q)$. Then it is not difficult to verify that the inner product restricted to W_m must be non-singular. Hence W_m splits off from $V_{p(t)}$ as an orthogonal direct summand. Since the complementary summand $W_m^{\perp}$ is clearly closed under the action of t, an easy induction completes the argument.

Proof that the hermitian space H^q *does not depend on the choice of* V^q. Let $V(q)$ denote the set of all $v \in V$ with $p(t)^q v = 0$. Then clearly $V^q/p(t)V^q$ is isomorphic to the quotient

$$V(q)/\big(V(q-1) + p(t)V(q+1)\big)$$

which is invariantly associated with (V, t). Also it is clear that the inner product $\langle v, s(t)^{q-1} w\rangle$ for v and w in $V(q)$ is symmetric and depends only on the residue classes of v and w modulo $V(q-1) + p(t)V(q+1)$. Denoting these residue classes by (v) and (w), and proceeding just as in § 1.1 we construct the required hermitian inner product $(v) \cdot (w)$.

Proof that the structure of H^q *determines the isomorphism class of* V^q *and of* $t|V^q$. Choose an orthogonal basis $(v_1), \ldots, (v_r)$ for H^q, and choose some representative $v_1 \in (v_1)$. As basis for the subspace $F[t]v_1 \subset V^q$ we will use the vectors $t^i s(t)^j v_1$ with $0 \leqq i < 2d$ and $0 \leqq j < q$. We wish to choose the representative vector v_1 so that the matrix of inner products

$$\langle t^i s(t)^j v_1, t^{i'} s(t)^{j'} v_1\rangle = \langle t^{|i-i'|} s(t)^{j+j'} v_1, v_1\rangle$$

takes on as simple a form as possible. In fact, if the characteristic is $\neq 2$, we will choose v_1 so that this inner product is zero whenever

$$|i - i'| < d \quad \text{and} \quad j + j' \neq q - 1.$$

The remaining inner products can then be computed as follows (setting $i' = j' = 0$ to simplify the notation). If $j = q-1$ we have

$$\langle t^i s(t)^{q-1} v_1, v_1\rangle = \operatorname{trace}(\tau^i k_1), \qquad \text{where } k_1 = (v_1) \cdot (v_1);$$

while if $i \geqq d$ then the element $t^i + t^{-i}$ in the ring $F[t + t^{-1}]$ can be expressed as a multiple of $s(t)$ plus a remainder. The inner product $\langle t^i s(t)^j v_1, v_1\rangle$ can then be computed by induction on i.

Choice of a preferred representative in (v_1) *assuming that* F *has characteristic* $\neq 2$. Starting with some arbitrarily chosen representative v_1, first set

$$v_1' = v_1 + a(t)s(t)v_1$$

where $a(t)$ is a polynomial to be selected later. Note that the inner product $\langle t^i s(t)^{q-2} v_1', v_1' \rangle$ is equal to $\langle t^i s(t)^{q-2} v_1, v_1 \rangle$ plus the correction term

$$\langle t^i s(t)^{q-1}(a(t)+a(t^{-1}))v_1, v_1\rangle = \operatorname{trace}_{E/F}(\tau^i(a(\tau)+a(\bar{\tau}))k_1)$$
$$= \operatorname{trace}_{K/F}((\tau^i+\bar{\tau}^i)(a(\tau)+a(\bar{\tau}))k_1).$$

Since the elements $(\tau^i+\bar{\tau}^i)k_1$ with $0 \leqq i < d$ form a basis for K over F, there exists one and only one element $a(\tau)+a(\bar{\tau})$ of K so that this trace is equal to $-\langle t^i s(t)^{q-2} v_1, v_1\rangle$ for each such i. Now choosing a corresponding polynomial $a(t)$, we have constructed a representative $v_1' \in (v_1)$ so that

$$\langle t^i s(t)^{q-2} v_1', v_1' \rangle = 0$$

for $0 \leqq i < d$.

Next we can choose a polynomial $b(t)$ so that the vector

$$v_1'' = v_1' + b(t)s(t)^2 v_1'$$

satisfies the identity

$$\langle t^i s(t)^j v_1'', v_1'' \rangle = 0$$

for $0 \leqq i < d$ and for $j = q-2, q-3$. Then add a multiple of $s(t)^3$ to v_1'' and so on, continuing inductively until we obtain the required representative for (v_1).

Thus the entire inner product structure and $F[t]$-module structure of the space $F[t]v_1$ is completely determined by the single field element $k_1 \in K$. Note in particular that the inner product restricted to $F[t]$-

orthogonal complement. Choosing a representative for (v_2) in the orthogonal complement and continuing inductively, this proves that the structure of V^q and $t|V^q$ is completely determined by the field elements $k_1, \ldots, k_r$; and hence is completely determined by the hermitian space H^q.

This proves Theorem 3.3 (except in characteristic 2), and also proves that the splitting in Theorem 3.2 is unique up to isomorphism.

In characteristic 2, only a slight modification of this argument is

Conversely, given any separable symmetric irreducible polynomial $p(t)$ and any hermitian space H^q over $F[t]/p(t)F[t]$, it can be verified that the matrices constructed in this way do indeed yield a quadratic space V^q with an isometry t so that V^q is free when considered as a module over $F[t]/p(t)^q F[t]$. This completes the discussion of Case 1.

The proofs in Case 2 are similar, and will be omitted. (Compare Cikunov [5].)

References

1. Artin, E., and J. Tate: Class field theory. New York: Benjamin 1967.
2. Cartan, H., and S. Eilenberg: Homological algebra. Princeton Univ. Press 1956.
3. Cikunov, I. K.: The structure of isometric transformations of a symplectic or orthogonal vector space. Dokl. Akad. Nauk SSSR **165**, 500 – 501 (1965), or Soviet Math. Dokl. **6**, 1479 – 1481 (1965).
4. – Structure of isometric transformations of a symplectic or orthogonal vector space [Russian]. Ukrain. Mat. Ž. **18**, No. 4, 79 – 93 (1966).
5. – A class of isometric transformations of a symplectic or orthogonal vector space [Russian]. Ukrain. Mat. Ž. **18**, No. 5, 122 – 127 (1966).
6. – On the structure of isometric transformations of symplectic and orthogonal vector spaces over a finite field $GF(q)$ [Russian, English summary], Algebra and Math. Logic: Studies in Algebra [Russian], 72 – 97, Izdat. Kiev Univ. 1966.
7. Jacobson, N.: A note on hermitian forms. Bull. Amer. Math. Soc. **46**, 264 – 268 (1940).
8. Landherr, W.: Äquivalenz Hermitescher Formen über einem beliebigen algebraischen Zahlkörper. Abh. Math. Sem. Hamburg Univ. **11**, 245 – 248 (1935).
9. Lang, S.: Algebra. Reading, Mass.: Addison-Wesley 1965.
10. Levine, J.: Knot cobordism groups in codimension two. Comment. Math. Helv. **44**, 229 – 244 (1969).
11. – Invariants of knot cobordism. Inventiones math. **8**, 98–110 (1969).
12. Milnor, J.: Infinite cyclic coverings, pp. 115 – 133 of Conference on the Topology of Manifolds, ed. J. G. Hocking, Boston: Prindle, Weber and Schmidt 1968.
13. O'Meara, O. T.: Introduction to quadratic forms. Berlin-Göttingen-Heidelberg: Springer 1963.
14. van der Waerden, B. L.: Modern algebra I. New York: Ungar 1949.
15. Wall, G. E.: On the conjugacy classes in the unitary, symplectic and orthogonal groups. Journ. Australian Math. Soc. **3**, 1 – 62 (1963).
16. Williamson, J.: Normal matrices over an arbitrary field of characteristic zero. Amer. J. Math. **61**, 335 – 356 (1939).

John Milnor
Massachusetts Institute of Technology
Department of Mathematics
Cambridge, Mass. 02139, USA

(Received March 15, 1969)